Report *based on* discussions *with the*

Security for Business Innovation Council

An industry initiative sponsored by RSA

ABN AMRO
DR. MARTIJN DEKKER, *Senior Vice President, Chief Information Security Officer*

ADP INC.
ROLAND CLOUTIER, *Vice President, Chief Security Officer*

AIRTEL
FELIX MOHAN, *Senior Vice President and Chief Information Security Officer*

THE COCA-COLA COMPANY
RENEE GUTTMANN, *Chief Information Security Officer*

CSO CONFIDENTIAL
PROFESSOR PAUL DOREY, *Founder and Director; Former Chief Information Security Officer, BP*

EBAY
DAVE CULLINANE, *Chief Information Security Officer and Vice President, Global Fraud, Risk & Security*

EMC
DAVE MARTIN, *Chief Security Officer*

GENZYME
DAVID KENT, *Vice President, Global Risk and Business Resources*

HDFC BANK
VISHAL SALVI, *Chief Information Security Officer and Senior Vice President*

HSBC HOLDINGS plc
ROBERT RODGER, *Group Head of Infrastructure Security*

JOHNSON & JOHNSON
MARENE N. ALLISON, *Worldwide Vice President of Information Security*

JPMORGAN CHASE
ANISH BHIMANI, *Chief Information Risk Officer*

NOKIA
PETRI KUIVALA, *Chief Information Security Officer*

NORTHROP GRUMMAN
TIM MCKNIGHT, *Vice President and Chief Information Security Officer*

SAP AG
RALPH SALOMON, *Vice President, IT Security & Risk Office, Global IT*

T-MOBILE USA
WILLIAM BONI, *Corporate Information Security Officer (CISO), VP Enterprise Information Security*

WITH GUEST CONTRIBUTOR:
WILLIAM PELGRIN, *President & CEO, Center for Internet Security; Chair, Multi-State Information Sharing and Analysis Center (MS-ISAC); and Immediate Past Chair, National Council of ISACs (NCI)*

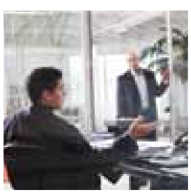
GETTING AHEAD OF ADVANCED THREATS

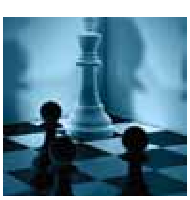
Achieving Intelligence-Driven Information Security

RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES

INSIDE THIS REPORT:

Contents





Report Highlights

IN TODAY'S THREAT landscape, organizations worldwide face a growing number of sophisticated cyber adversaries.

"ADVANCED THREATS" ARE increasingly targeting corporations and governments in order to conduct industrial espionage, undermine business and financial operations, and/or sabotage infrastructure.

THE HARD TRUTH IS MOST organizations don't know enough about the threats or their own security posture to defend themselves adequately against the rising tide of cyber attacks.

THE TIME HAS COME WHEN successful defense requires evolving past conventional approaches in information security.

A NEW APPROACH IS NEEDED. Called "intelligence-driven information security," this approach includes:

- The consistent collection of reliable cyber-risk data from a range of government, industry, commercial, and internal sources to gain a more complete understanding of risks and exposures.
- Ongoing research on prospective cyber adversaries to develop knowledge of attack motivations, favored techniques, and known activities.
- The growth of new skills within the information team focused on the production of intelligence.
- Full visibility into actual conditions within IT environments, including insight that can identify normal versus abnormal system and end-user behavior.
- A process for efficient analysis, fusion, and management of cyber-risk data from multiple sources to develop actionable intelligence.
- Practices to share useful threat information such as attack indicators with other organizations.
- Informed risk decisions and defensive strategies based on comprehensive knowledge of the threats and the organization's own security posture.

THE VISION IS TO HARNESS THE power of information to prevent, detect, and ultimately *predict* attacks.

THE VALUE PROPOSITION IS clear. By maximizing the use of available information, the organization can create and implement more precise defensive strategies against evolving threats. Security will not only improve but also become more cost-effective because it will be targeted at countering the most significant threats and protecting the most strategic assets.

NOTE ON THE SCOPE OF THIS REPORT:

THIS REPORT is focused on the collection and analysis of cyber-risk data. However, many organizations' intelligence programs may include a broader set of data. For example, they may include physical-security data (building access, travel), manufacturing supply chain risks (availability, delivery), and/or data on competitors (financials, product developments). Although the scope of this report is cyber-risk intelligence, the goal for some organizations' intelligence programs is to build a complete picture of operational risks.

THIS REPORT PROVIDES A SIX-step roadmap for achieving intelligence-driven information security.

THE GUIDANCE ANSWERS critical questions such as:

- What are the basic requirements for building an intelligence capability?
- What does it take to develop broad organizational support and obtain funding?
- What is the skill set required of a cyber-risk intelligence team?
- What are the best sources of data?
- How can an organization design a process that will consistently produce actionable intelligence and the right defensive strategies?
- What type of automation can help create efficiencies for handling large volumes of data?

A CRITICAL ASPECT OF achieving intelligence-driven information security is sharing cyber-risk data with other organizations. But there are many significant challenges to creating information-sharing mechanisms.

FORTUNATELY, THERE IS A growing number of industry and government-led initiatives as well as public/private partnerships that are working to enable large-scale data exchange.

1 Introduction: The Need to Know

Corporations and governments worldwide are increasingly targeted by cyber adversaries with a range of goals from political activism and sabotage to intellectual-property theft and financial gain. As cyber attacks intensify and tactics rapidly evolve, organizations could find the escalating threat landscape overwhelming their abilities to manage the risks.

The hard truth is most organizations don't know enough about the threats or their own security posture to defend themselves adequately. For example, they can't see signs of an attack because they haven't sufficiently analyzed data on the latest attack techniques. They can't identify malicious activity because they haven't developed baselines for normal activity.

Today's dedicated adversaries have the means to evade commonly used defenses such as signature-based detection. In the era of advanced threats, greater situational awareness is essential to detect and mitigate cyber attacks effectively. Organizations need to obtain the latest data on threats, relate that to real-time insights into their dynamic IT and business environments, determine what's relevant, make risk decisions, and take defensive action.

Intelligence gathering and analysis have become essential capabilities for a successful information-security program, yet most enterprise IT

Cyber-risk intelligence is table stakes in 21st-century commerce. If you want Internet access to a global array of customers and suppliers, then you have to invest in developing the intelligence capabilities to defend against global threats.

WILLIAM BONI,
Corporate Information Security Officer (CISO),
VP Enterprise Information Security,
T-Mobile USA

security organizations have not been built with this objective in mind. In fact, many cyber adversaries have developed better intelligence capabilities than their targets.

While many organizations may have access to the right data, they may not be set up to make use of it. Internal data collection is often tuned for compliance reporting not cyber-threat analysis. There are many external sources of threat data available, such as government channels, industry associations, and commercial data feeds. However, most organizations are not fully utilizing these sources. In addition, in order to maximize their value, many current information-sharing mechanisms would require increased participation.

This ninth report of the Security for Business Innovation Council (SBIC) features the perspectives of top security leaders from Global 1000 companies, as well as a guest contributor from the U.S. National Council of ISACs (NCI). Today's threats are dynamic and increasing in sophistication, requiring a fresh and more comprehensive approach to defense. This report provides a playbook for creating a new approach based on building an organizational competency in cyber-risk intelligence and fully leveraging data from internal and external sources. Advanced threats represent an escalating risk to business innovation. This report lays out a roadmap to achieving intelligence-driven information security in order to get ahead of the threats and protect critical information assets.

2 What Do Organizations Need to Know?

Organizations need to understand the cyber threats they face and their security posture against those threats. For this report, "cyber-risk intelligence" is defined as "knowledge about cyber adversaries and their methods combined with knowledge about an organization's security posture against those adversaries and their methods." The goal is to produce "actionable intelligence," which is knowledge that enables an organization to make risk decisions and take action. To gain that knowledge, organizations must take input data and process it. In this report, the term for that input data is "cyber-risk data" and is broadly defined as "data that is collected and analyzed in order to prevent, detect, predict, and defend against cyber attacks."

Sample code from the Ice IX Trojan which was derived from the leaked code of the prolific banker Trojan, ZeuS.

Cyber-risk data

Data used to produce intelligence is available from a range of sources either external or internal to the organization. Open source is obtained from publicly available sources such as websites, as opposed to data from classified sources such as national-security agencies. It comes in many formats, such as word-of-mouth, emails, news feeds, automated data streams, output of numerous internal and external sensing platforms, and custom research. Some types, such as a list of IP addresses on a watch list, are generally applicable to all organizations. Other types are unique to one organization, for example notification that it is being targeted by a particular group.

To understand the intelligence process, it is important to recognize the distinction between "intelligence" and "data" or "information." Data received from various sources as described above is typically raw data that needs to be reviewed, analyzed, and put in context in order to develop intelligence which can then be used to make risk decisions.

Not all organizations will choose to collect all types of data from all sources. Some data may not be considered useful or may not be cost-effective to obtain. Other data may be deemed useful but not feasible to acquire yet, because an organization's processes and/or technology for handling that particular type of data still need to be set up and integrated.

Moreover, collecting more and more data is not the end goal. Having volumes of unanalyzed or unused data is of no value to an organization. Ultimately, for the data to be valuable, the organization must be able to apply it defensively, for immediate action in combatting a current or imminent cyber attack and/or for informing defensive strategies. As discussed in subsequent sections of this report, the defensive application must be determined through analysis, including fusing the data with other relevant facts and making a risk decision.

Charts 1 to 5 present categories of cyber-risk data including examples of sources, formats, and potential defensive applications. The charts reflect some typical examples of data formats that are used today. However, it should be acknowledged that over time, for an intelligence program to be effective, many categories of data must become machine-readable. Currently, many organizations are heavily dependent on highly skilled analysts to process, for example, long lists of text. Instead, it would make sense to automate the processing of basic data, freeing up the analysts' time to do actual analyzing.

Charts 1-5: Categories of Cyber-Risk Data with Examples

Each category answers a different question about the threats and an organization's security posture against them

ACRONYMS USED *in charts:*

CERT: Computer Emergency Response Team
ISAC: Information Sharing and Analysis Center
WARP: Warning, Advice, and Reporting Point
MSSP: Managed Security Service Provider
DDoS: Dedicated Denial of Service
NVD: National Vulnerability Database
SQL: Structured Query Language
SIEM: Security Information and Event Management
DLP: Data Loss Prevention
GRC: Governance, Risk, and Compliance

CHART 1

INPUT DATA ON CYBER ADVERSARIES AND THEIR METHODS – EXTERNAL SOURCES

CYBER-ATTACK INDICATORS

WHAT SIGNS ARE OTHER ORGANIZATIONS SEEING THAT COULD BE USED BY US TO PREVENT, DETECT, OR PREDICT A CYBER ATTACK?

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
Description of spear-phishing emails	• Open source • Government sources • Industry partners • Sector ISACs	• Email alert	• Identify and block these emails
Lists of domains hosting malware	• Open source • Government sources • Industry partners • Sector ISACs	• Email alert • Listserv	• Identify and block traffic to these domains
List of black-listed IP addresses	• Open source • Government sources • Industry partners • Sector ISACs • Vendor lists	• Email alert • Threat feed	• Identify and block traffic to these IP addresses
Set of binaries used by attackers	• Vendor lists • Tool output • MSSP • Cloud service	• Threat feed	• Identify and remove malware

CYBER-ATTACK TECHNIQUES

WHAT HAVE OTHERS LEARNED ABOUT ATTACK TECHNIQUES THAT COULD BE USED TO PREVENT, DETECT, PREDICT, OR DEFEND AGAINST CYBER ATTACKS?

Description of attack pattern using multiple vectors including social engineering	• Law enforcement cyber-intelligence agencies • Industry partners	• Briefing • In-person meeting	• Update detection methods and implement ways to block this attack technique
Description of new exploit involving mobile devices	• Government CERTs • Vendor community	• Email alert	• Update controls on mobile devices

CHART 1 (CONTINUED)

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
CYBER ATTACKERS' MOTIVES AND TARGETS			
WHAT ARE OUR ACTUAL OR POTENTIAL CYBER ADVERSARIES TRYING TO ACCOMPLISH?			
Explanation of trend whereby attackers select corporations with certain policies to hit with aggressive DDoS attacks	• Government agencies • Law enforcement cyber-intelligence agencies • Industry partners	• Information on hacktivism	• Shore-up DDoS defenses
Evidence that attackers are pursuing company's intellectual property such as new product plans or proprietary financial figures	• Commercial threat-intelligence services • Law enforcement cyber-intelligence agencies	• Threat feed • Custom research	• Increase protection of targeted assets
Evidence that nation-state operatives are stealing proprietary information from companies in the same industry	• Government agencies • Commercial threat-intelligence services • Law enforcement cyber-intelligence agencies	• Classified briefing • Custom research • In-person meeting	• Increase protection of targeted assets
CYBER ATTACKERS' IDENTITIES			
WHO ARE OUR ACTUAL OR POTENTIAL ATTACKERS?			
Specific information on attackers' identities: name and location of particular criminal groups which are targeting the company	• Government agencies • Commercial threat-intelligence services • Law enforcement cyber-intelligence agencies	• Classified briefing • Custom research • In-person meeting	• Learn to recognize specific attackers' footprints

CHART 2

INPUT DATA ON CYBER INCIDENTS AND COUNTER MEASURES – EXTERNAL SOURCES

EXTERNAL INCIDENT INFORMATION			
WHAT CAN WE LEARN FROM INCIDENTS AT OTHER ORGANIZATIONS TO PREVENT, DETECT, PREDICT, OR DEFEND AGAINST CYBER ATTACKS?			
Details regarding company in the same industry disclosing massive data breach	• Media • Sector ISACs • Industry partners	• News websites • Email alert • Information portals	• Integrate lessons learned into defensive strategies
COUNTER-MEASURES AND DEFENSIVE TECHNIQUES			
WHAT BEST PRACTICES CAN WE LEARN FROM OTHER ORGANIZATIONS TO DEFEND AGAINST CYBER ATTACKS?			
Description of new procedures for protecting admin accounts from hijacking	• Peer organizations • Sector ISACs	• Email alert • Information portals • In-person meeting	• Implement new controls around admin accounts

CHART 3

INPUT DATA ON AN ORGANIZATION'S SECURITY POSTURE RELATIVE TO CYBER THREATS – EXTERNAL SOURCES

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
GENERAL VULNERABILITIES			
ARE THERE VULNERABILITIES IN SOFTWARE/HARDWARE THAT COULD MAKE US PRONE TO ATTACK?			
Description of operating system vulnerability	• Government CERTs • Vendor community	• NVD data feed	• Implement patch
Description of SQL injection vulnerability	• Sector ISACs • Vendor community • Commercial threat-intelligence services	• Email alert	• Update application
SPECIFIC VULNERABILITIES			
ARE THERE SPECIFIC VULNERABILITIES REGARDING OUR SYSTEMS THAT COULD MAKE US PRONE TO ATTACK?			
Discovery of a set of the company's access credentials on hacker websites	• Cybercrime-intelligence service vendors	• Custom research	• Update credentials

"The threat can be broken down into three components: intent, opportunity, and capability. Organizations need to know, 'What is the intent of adversaries? What are the opportunities available to them? And what capabilities do they have to exploit the opportunities?'"

FELIX MOHAN, Senior Vice President and Chief Information Security Officer, Airtel

CHART 4

INPUT DATA ON AN ORGANIZATION'S SECURITY POSTURE RELATIVE TO CYBER THREATS – INTERNAL SOURCES

INFORMATION-ASSETS INVENTORY

WHAT ARE OUR MOST IMPORTANT INFORMATION ASSETS TO PROTECT AND WHERE ARE THEY LOCATED?

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
Periodic inventory of high-value assets including asset type, relative value to the organization, location, and security exposure	• Risk-management team	• Internal report	• Establish status and location of systems containing IP to ensure adequate protection

EMPLOYEE OBSERVATIONS

WHAT SUSPICIOUS ACTIVITIES ARE EMPLOYEES OBSERVING THAT COULD BE SIGNS OF A CURRENT OR FUTURE CYBER ATTACK?

Reports of phone calls being received by members of the R&D team asking about colleagues	• Employees' communications • Employees' entries into knowledge-management system	• Emails to Security • Knowledge-management system alert	• Determine attackers' methods and increase security controls to protect targeted assets

BUSINESS STRATEGY

WHAT ELEMENTS OF OUR STRATEGY WOULD CREATE POSSIBLE OPPORTUNITIES FOR A CURRENT OR FUTURE CYBER ATTACK?

Information regarding outsourcing of business processes to external providers	• Business/mission owners	• Internal reporting	• Implement real-time monitoring of new business partners' IT systems and security controls
Notice that company will be undergoing merger negotiations	• Finance department • Legal department	• Confidential memo to Security	• Implement increased monitoring and controls around privileged users involved in negotiations
Evidence that reduction in workforce is creating disgruntled employees	• Human resources department	• Confidential memo to Security	• Implement increased monitoring and controls for employees with access to protected assets

INTERNAL INCIDENT INFORMATION

WHAT CAN WE LEARN FROM PAST CYBER INCIDENTS TO PREVENT, DETECT, PREDICT, OR DEFEND AGAINST FUTURE ONES?

Report regarding malware that was detected and remediated	• Security-operations team	• Incident report	• Integrate lessons learned and strategy to shorten kill chain in the future

CHART 5

INPUT DATA ON AN ORGANIZATION'S SECURITY POSTURE RELATIVE TO THE CYBER THREATS – IT AND SECURITY SOURCES

CYBER-RISK INFRASTRUCTURE EVENTS

ARE EVENTS WITHIN THE SECURITY INFRASTRUCTURE SIGNS OF A CURRENT OR FUTURE ATTACK?

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
Warning that unauthorized connections to servers attempted	• Correlated SIEM events	• System alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further
Signs of command and control activity, data exfiltration, or other lateral movement	• Full packet capture, DLP or SIEM events	• System alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further

END-USER AND SYSTEM BEHAVIOR DATA

IS END-USER OR SYSTEM BEHAVIOR SIGNALING A POSSIBLE CURRENT OR FUTURE CYBER ATTACK?

Sign of an unusual admin remote login – comparison with baseline	• Authentication log • SIEM	• Log analysis alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further
Sign of increasing password resets – notable trend	• Full packet capture • Application logs	• System alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further
Sign of unusual data movement – traffic outside of the norm or to unusual destinations	• Full packet capture • Application logs	• System alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further

STATUS OF CONTROLS

WHAT IS THE CONDITION OF OUR CURRENT CYBER DEFENSES?

Notification that major business line did not complete mandatory password resets for all users	• GRC system	• System report	• Increase monitoring on specific systems until remediated
Notification of upload-policy violations	• DLP system	• System report	• Increase monitoring on specific systems and investigate further

3 Time for a New Approach

Intelligence-Driven Information Security

Depending on the maturity of the information-security program, organizations may already integrate cyber-risk data into their defensive strategies. For example, it is fairly common for organizations to have a basic vulnerability-management program for collecting data on software and hardware vulnerabilities and ensuring systems are adequately patched and updated. Many security professionals read industry publications such as vendor reports on malware and data breaches and consider this information when creating security strategies.

For most information-security programs, however, data collection and analysis are not strong suits. Collection from external sources is often fragmented and not integrated with internal data sources. And although many organizations collect reams of data from applications and security systems, they aren't harvesting and analyzing the data to gain an understanding of their environment, such as developing baselines for normal activity. Instead, much of the data ends up as dead logs.

Most organizations do not have a concerted effort to collect, amalgamate, analyze, operationalize, and manage cyber-risk data in order to develop intelligence. Yet more and more organizations need this capability in order to defend against advanced threats.

DEFINITION

Intelligence-driven information security

Developing real-time knowledge on threats and the organization's posture against those threats in order to prevent, detect, and/or predict attacks, make risk decisions, optimize defensive strategies, and enable action.

There is mounting evidence that organizations in a wide range of industries are increasingly targeted by sophisticated adversaries. For example, a recent report by the U.S. Office of the National Counterintelligence Executive[1] states, "The pace of foreign economic collection and industrial espionage activities against major U.S. corporations and U.S. government agencies is accelerating." A major reason is the accessibility of sensitive data in cyberspace. The report also indicates that many companies are unaware when their sensitive data is pilfered. Further, it suggests that areas of great interest to cyber spies include information and communications technology, natural resources, defense, energy, and healthcare/pharmaceuticals.

> *"It can be hard to digest having to develop a multi-year plan to learn who your adversaries are and how they're going to steal from you. Quarter-by-quarter, you may not see any losses. It could be years until you see the losses – when all of a sudden, out of the blue, a company in another part of the world becomes the leader in your space, having subsidized itself with your R&D investments."*

TIM MCKNIGHT
Vice President and Chief Information Security Officer, Northrop Grumman

[1] "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," Office of the Director of National Intelligence/Office of the National Counterintelligence Executive, October 2011

Other studies indicate that companies across the globe are being targeted. For example, the Enterprise Strategy Group surveyed companies in the U.S. and Europe regarding advanced persistent threats (APTs) and found that 59% of security professionals surveyed at U.S. companies[2] and 63% of those at European companies[3] believe it is "highly likely" or "likely" that their organizations have been APT targets.

In today's threat landscape, organizations face targeted, complex, multi-modal attacks which can be carried out over periods of time. They need to fuse together data drawn from multiple sources to effectively detect and mitigate attacks. They need comprehensive, accurate, and timely information to make informed decisions about defensive strategies. The time has come when successful defense requires evolving past conventional approaches in information security to developing competencies in data fusion, knowledge management, and analytics.

Change of mind-set required

Currently, many information-security programs are compliance-led: Decision making about defensive strategies is based on the audit cycle or the need to simply meet a regulatory baseline. Another common approach is incident-led: Decision making is based on day-to-day fire-fighting. What is needed is an intelligence-driven approach, whereby decisions are made based on real-time knowledge regarding the cyber adversaries and their attack methods, and the organization's security posture against them.

Some security professionals may see gaining intelligence about potential cyber threats as the government's responsibility, but it is unrealistic for any national government to take on threat analysis for each specific organization, especially in the private sector. Governments don't have the resources nor do they have the mandate. It is the organization itself that knows its own business or mission, market position, asset valuation, and vulnerabilities and can make the best determination of the cyber threats it confronts. However, governments can play an important role in providing cyber-risk intelligence and fostering information sharing.

Building an intelligence capability will also require developing a counterintelligence and operational security mind-set among the entire extended security team. This means seeing one's own organization from the perspective of the adversaries who are targeting it, being able to understand their tools and techniques, and identifying potential vulnerabilities before they do.

Key features

An intelligence capability applies expertise, processes, and tools to:

- consistently collect the right data from the right sources
- efficiently amalgamate, analyze, and manage the data
- develop knowledge and produce actionable intelligence
- make risk decisions and take action by modifying controls or planning new defenses
- share relevant pieces of data such as attack indicators with other organizations

Building this capability will require investments in people, process, and technology. Of course, not every organization has to achieve the intelligence capability of a national-security agency. But there is a large spectrum between having no accountability for intelligence and achieving the level required by a highly specialized threat environment. Every organization will need to determine its level of investment based on the particular threats it faces, the value of the assets it needs to protect, and its risk profile.

Organizations don't have to make huge investments to get started. They can start today using existing personnel, for example, to improve the collection and analysis of log data or to integrate open source threat intelligence. Over time, a key element will be automation to help decrease manual processes. Otherwise the collection and analysis of greater amounts of data could become onerous and resource-intensive. Another important aspect is having an agile program whereby protection methods can be dynamically put into place in response to the intelligence.

The vision is to harness the power of information to prevent, detect, and ultimately predict attacks. Getting ahead of threats requires an ability to see what's coming in order to determine appropriate action before an attack happens.

[2] *U.S. Advanced Persistent Threat Analysis: Awareness, Response, and Readiness among Enterprise Organizations, Enterprise Strategy Group, October 2011*

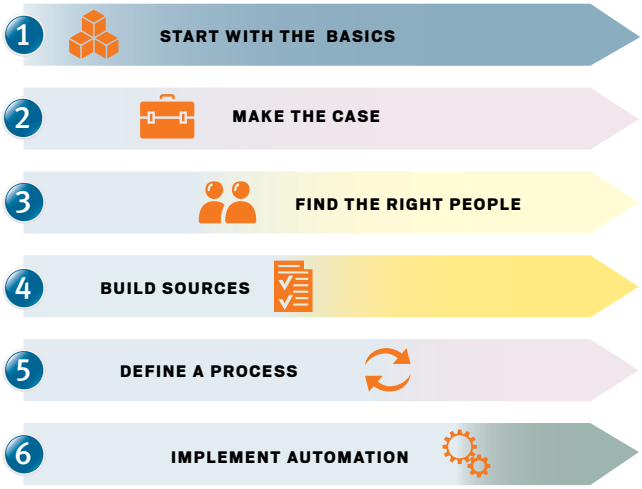
[3] *Western Europe Advanced Persistent Threat (APT) Survey, Enterprise Strategy Group, October 2011*

4 Roadmap to Intelligence-Driven Information Security

"If you're really serious about having an intelligence-driven program, you have to have the resources and a process for risk decision-making that enable rapid changes to your protection platform. You can have all the intelligence in the world, but if you're not going to do anything with it, don't go down this road because it's a lot of wasted effort."

ROLAND CLOUTIER
Vice President, Chief Security Officer, Automatic Data Processing, Inc.

The following roadmap lays out a basic route for developing an intelligence-driven approach to information security. While the exact route an organization takes will depend on its own unique circumstances, this roadmap offers some general direction and things to consider at various stages. The steps will likely be parallel endeavors but the focus of the program will move from one step to the next in sequence.



Step 1: Start with the Basics

Inventory of strategic assets

A fundamental requirement of intelligence-driven information security is to have an inventory of strategic assets since it will be impossible to collect data on everything and protect everything. Organizations need to know what are the most important assets to protect and where they are located. Over the past several years, many organizations have established an inventory of assets through a data-discovery process as part of their risk and compliance programs.

Incident-response process

Another requirement is a Security Operations Center (SOC) or Computer Emergency Response Team (CERT), either internally managed or run by a managed security services provider. To be ready to take on an intelligence program, the organization needs to have a foundation in place for monitoring the network for intrusions and a workflow process for responding to incidents. Ideally, this is a systematic process with well-defined roles.

Risk assessment

Organizations must also do a risk assessment. This involves determining the value of protected information assets, identifying potential sources of harm to those assets (threat assessment), determining the extent of existing vulnerabilities (vulnerability assessment), and evaluating the probability that the vulnerabilities could be successfully exploited and the potential impact to the organization. There are several good sources, including the National Institute for Science and Technology (NIST) and the SANS Institute, which provide detailed guidance on how to perform threat, vulnerability, and risk assessments.

Many organizations already routinely perform risk assessments as part of their security program. As the intelligence program progresses, there will be more data and better understanding which can be fed into ongoing risk assessments. But it is essential for an organization to begin with a basic understanding of the threats it faces and its risk posture.

"You need to align the intelligence process with your risk-management process. How the company identifies and measures risk needs to be understood and agreed to across the organization."

RALPH SALOMON
Vice President, IT Security & Risk Office, Global IT, SAP AG

Step 2: Make the Case

An essential component of developing an intelligence capability is communicating the benefits to executive management and key stakeholders in order to garner support and funding as well as to ensure ongoing enterprise-wide involvement in the effort. To be successful, intelligence-driven security must be an enterprise-wide core competency.

The value proposition

The main benefit is that the organization will be much better protected. By maximizing the use of available information, the organization can create and implement more precise defensive strategies against evolving threats.

Security will not only improve but also become more cost-effective because it will be targeted at countering the most significant threats and protecting the most strategic assets. Knowledge will enable the security team to perform fact-based prioritization. They will know how to concentrate their efforts and where to make the right investments in controls.

An intelligence-driven approach enables the security team to actually achieve proactive security management. By asking the right questions, combining multiple pieces of key external and internal data, looking at the bigger picture, and examining threats and vulnerabilities on a longer-term horizon, an intelligence-driven approach provides a view of more than single events or day-to-day incidents. It allows the team to see emerging attack patterns and developments over time, and eventually attain the necessary expertise to predict attacks and get ahead of the threats.

Key stakeholders

The communications strategy should not only convince key stakeholders of the benefits but also obtain their ongoing input to ensure success. Since intelligence-driven security is a new approach for many organizations, often it begins with developing a common language to use as the basis for discussions.

The list below suggests possible key stakeholders and how they might be involved in the intelligence effort:

- Executive Management and the Board
  Top-level support
  Risk decisions
- Finance
  Funding strategies
- Human Resources
  Employee-activity monitoring
- Corporate Security
  Collaborative data collection and investigations
- Procurement
  Third-party risk management
- Business/Mission Owners
  Identification of strategic assets and risks to business
- Production/Operations
  Identification of strategic assets and risks to manufacturing operations
- Business Risk Officers
  Enterprise view of risks

- Legal
  - Compliance to privacy regulations
  - Legal frameworks for obtaining threat data and sharing information with other organizations
  - Employee-activity monitoring
- IT
  - Programming, analytics, and automation
  - IT architecture and defensive strategies
  - IT operations for data sharing and service-level management

Opportunities for a "quick win"

Strategically, developing a fully deployed intelligence capability is going to be a multi-year effort. Typically, it makes sense for the security team to start small with the objective of quickly showing some good results. A "quick win" will help them gain the support and funding needed.

Since cyber attacks have recently received a lot of media attention, there is generally an elevated level of awareness among executive leaders and boards regarding the risks posed by advanced threats. Security teams can take advantage of this increased interest to propose cyber-risk intelligence projects as an integrated part of their security strategy. Leadership may be more open to providing the required funding and support than in the past. However, the proposed project must align to current top priorities and be able to deliver information that is specific and critical to the business. Information on vague, broad risks will not be useful.

More often than not, an intelligence-driven approach gets started because the security team seizes an opportunity. For example, a specific risk is identified as critical to the business and intelligence is proven to be very useful in mitigating that specific risk. Or a security incident occurs and intelligence is proven to be very useful in detecting the attack and/or reducing the risk of future incidents. Chart 6 provides some possible examples of opportunities, drawn from real-world experiences of Council members and their peers.

OPPORTUNITIES

6. EXAMPLES OF "QUICK WIN" OPPORTUNITIES TO SHOW VALUE

EXAMPLE OPPORTUNITY	PROJECT	RESULTS
Executives express concerns regarding hacktivism based on media reports. Many other organizations with a similar risk profile are being targeted by hacktivists and some have suffered shut-down of websites.	Data collection and analysis on this new class of threat: • A member of the incident-response team is assigned to do research on the likelihood of the company being targeted by hacktivists, impact, and how to defend against attacks • Based on research, specific adjustments made to DDoS defenses	Threat briefing to executives leads to support for more technology resources for threat analysis.
A critical component of the organization's business strategy depends on partnering with a new strategic partner.	Data collection and analysis on a potential business partner: • Short engagement with a threat-intelligence service to do research on potential threats to the business partner and the relationship • Based on research, specific recommendations are made regarding security requirements for doing business with the partner	Threat briefing to executives leads to support for more funding for threat-intelligence services
An insider incident involving systems containing IP leads to the awareness for increased protection of particular information assets.	Data collection and analysis on internal environment: • Security team requests assistance from business-intelligence team in developing baselines for end-user behavior in accessing a set of critical systems • Baselines established • Able to monitor activity on those systems for anomalies	Security team has support of organization to expand the number of systems for which to develop baselines of end-user behavior
A series of suspicious events leads to concern that certain systems have been compromised.	Use of external threat data • A short engagement with a threat-discovery service to monitor outgoing communications for signs of attack based on the vendor's attack-indicator database • A botnet is detected and remediated	Security team has support of organization to expand the number of systems for which to develop baselines of end-user behavior

PETRI KUIVALA
Chief Information Security Officer, Nokia

"In many organizations, improvements in security happen when there are incidents. It's human nature. Management will listen to the security team and agree to improvements at other times but they seem to get more interested and provide funding when there is an incident."

Step 3: Find the Right People

The skill set for cyber-risk intelligence professionals is quite different from the traditional skill set within the security department. Historically, security professionals required technical skills such as system administration or network administration skills, but cyber-risk intelligence teams require a different set of skills which are focused on determining how attack techniques might be used against the organization's IT infrastructure. It is a relatively senior role that also requires an ability to evaluate risks and make reasoned judgement calls.

Analytical skills and experience are crucial in order to look at what appear to be unrelated pieces of data to draw linkages, uncover patterns, see trends, and make predictions. Knowing how to construct and refine analytical models and work with other professionals such as programmers are also necessary skills, as well as specific expertise in network- and system-behavior analysis.

One of the most important aspects of the role is building and maintaining good relationships. Communication and writing skills are essential, such as being able to craft messages for various audiences. Other facets of the job will require skills in designing and managing processes, developing procedures, and implementing tools for the intelligence program.

Being inquisitive and investigative are useful traits for performing research. Depending on the organization's threat level and objectives for the program, there may be a need for people on the intelligence team who have the skills to do active research such as working in "underground" channels in order to collect intelligence on the adversaries. This could require specialized technical knowledge and skills in foreign languages and cultures. However, most organizations that decide to pursue detailed information on adversaries and their specific plots turn to threat-intelligence services.

The advantages are that the threat-intelligence services already have established methodologies for active research and have amassed a wealth of experience working with a wide spectrum of clients. The drawbacks are that the services can be costly for smaller organizations and an external service provider may not have a deep understanding of each individual organization's business. If an organization works with a threat-intelligence service, internal team members must be able to define the search parameters so that the service provider can deliver relevant information and also be able to put the information provided in context.

The title for the emerging role of cyber-risk intelligence professional is "analyst." Job descriptions vary depending on the goals and maturity of the program as well as the organizational structure. A sample job description for a "Cyber-Risk Intelligence Analyst" is provided in the sidebar on page 16.

This could be challenging for a single individual to accomplish. One approach is to have a multi-disciplinary team, combining people who have the various requisite skills. Many organizations do not have the resources to build a large dedicated team, especially in the early stages of an intelligence program. Instead, they might start by forming a virtual team by getting people from various departments to spend some time looking at security threats from different angles. Or, they might designate existing security resources, for example enlist senior members of the team to allocate time

"Cyber-risk intelligence requires a skill set combining abilities to understand threats, the business environment, and security controls in order to determine the risks to the business and what controls would mitigate those risks."

DAVE MARTIN
Chief Security Officer, EMC Corporation

to cyber-intelligence functions. Over time, the organization may dedicate full-time resources and/or hire people.

Finding the right people can be a challenge. Since cyber-risk intelligence is an emerging discipline, the skills are not widely available yet. But there are several good potential sources, including developing people from within the existing incident-response or forensics team or hiring professionals with a background in federal law enforcement, military intelligence, or banking-fraud analysis. Depending on the organizational structure, the cyber-risk intelligence team could reside within the information-security department or in an enterprise intelligence "fusion center," which includes other analysts working in areas such as physical security, supply chain, and competitive intelligence.

> *"Intelligence is all about relationships. Most companies have tons of information internally but it's not being shared. They have tons of information accessible through their service providers but they're not asking the right questions. You need people who can create trusted communication channels to leverage all of these sources."*

MARENE N. ALLISON
Worldwide Vice President of Information Security, Johnson & Johnson

JOB DESCRIPTION: CYBER-RISK INTELLIGENCE ANALYST

- Determining sources of intelligence
- Ensuring consistent and effective collection of data from those sources
- Doing research
- Consuming information such as reading bulletins, memos, and reports
- Performing tests on the IT environment to check for attack indicators or known techniques
- Implementing automated methods of consuming data
- Analyzing information
  - *Constructing and refining analytical models and running analytical tools*
  - *Developing threat scenarios*
- Writing and presenting threat briefings for various audiences (daily, weekly, and quarterly briefings)
- Developing relationships and networks of contacts
  - *Internal such as IT team and business lines*
  - *External such as law enforcement, information-sharing associations, and peers at other companies*
- Developing trusted communication channels
- Building an end-to-end intelligence process
- Working with other teams to act on the intelligence, such as improving detection or defensive strategies

Step 4: Build Sources

Good sources of cyber-risk data depend on what information is sought. Based on the current knowledge of threats and the organization's security posture against them, the cyber-risk intelligence team needs to determine what additional data would help prevent, detect, or predict attacks.

For instance, the team may decide to improve the collection of cyber-attack indicators from external sources to increase the likelihood of catching a potential problem. There may be a surge of spear-phishing emails affecting one of the business units and the team wants to know if and when other units get hit. They may see potential for an APT-style attack and want to know who could be targeting them.

Once information requirements are determined, the team can seek out good sources. Various types and key factors are presented in Charts 7-11. Finding good sources is an ongoing process – information requirements need to be reviewed, current sources assessed to determine if they meet requirements, and new sources researched and evaluated. As well, as data is collected and analyzed, sources may need to be adapted on-the-fly. Even trusted sources could get things wrong. Keep in mind that sources vary significantly in quality and scope. Some of the best sources may cost very little and some of the worst may cost a lot. The value of the data from each source should be tracked so that, over time, the team can judge how good particular sources are.

Evaluation criteria

The cyber-risk intelligence team should not only consider the attributes of the source but also the organization's ability to make use of the data from that source. Questions include:

- How trustworthy is the source?
  - Does the source provide consistent, reliable, accurate, trustworthy data?
  - Are we able to effectively collect and consume data from this source?
  - Is the data machine-readable or does it require human intervention?
  - If it is machine-readable, what format is it in and do we have the right tools in place to use it in an automated fashion? (For example, could we integrate the data with our Security Information and Event Management (SIEM) system?)
  - If it requires human intervention, do we have the right people to review it, analyze it, and/or use it to manually perform tests on our environment?
  - Do we have a data-management process that can ensure the confidentiality and integrity of the data and handle sensitive data (for example, if the source can't be quoted)?
- If the source is our internal IT infrastructure, do we have the right tools to capture or generate the right data?
  - Could we reconfigure logging or correlation rules to get the data we need? Or would we need additional tools to generate the required data?
- Do we have the time to invest in fostering the relationships that may be required to work with this source? (Internal or external sources often require relationships.)

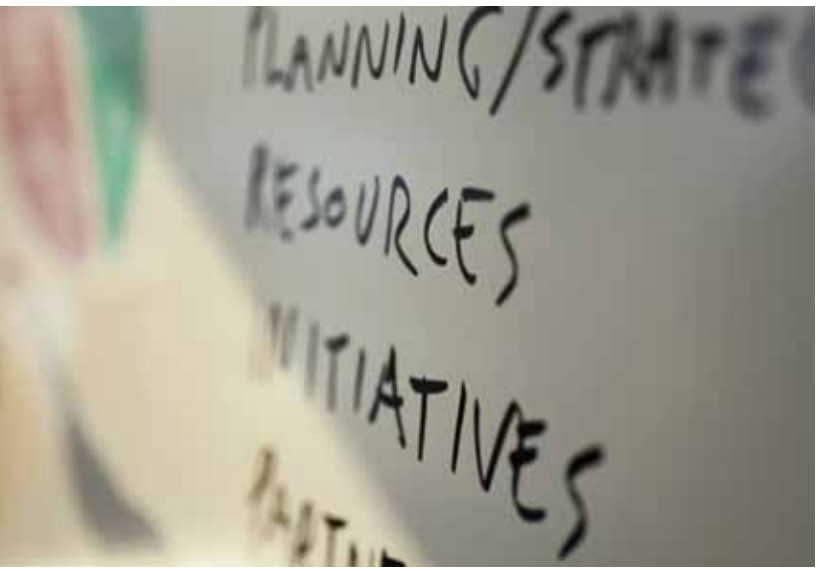
"If something happens at your organization, the first question you'll ask is, 'Is it just me or is everybody else getting hit with this attack?' You can't answer that for yourself. And it takes too long to call 20 of your closest friends. You've got to be part of a larger gene pool to get an immediate answer to that question."

RENEE GUTTMANN
Chief Information Security Officer,
The Coca-Cola Company

- What are the costs involved?
  - Are there up-front costs to receive the information? Is there a membership fee? Subscription-based fee? Service fee? Would it be a custom engagement?
  - How many personnel will it take to collect and make use of the data?
- If it's an information-sharing arrangement, are the required processes in place?
  - Do we trust that the data we provide to others will be handled with care, for example be kept confidential or de-identified if distributed?
  - Do we have a policy for determining what data will be shared with external entities and how?
  - Have we established the legal frameworks, rules of engagement, and/or agreements (NDA) for working with this source?
  - How much time and effort will it require to package up our data in order to share with external entities?
- Is the data provided by this source actionable?
  - Or is it too vague and broad to use?
- Is the data additive?
  - Does it provide corroborating information?
  - Or is it redundant data that we already obtain from another source?

> *Build your source material – whether from government or commercial sources, individuals in your organization, or business-intelligence processes. Your sources have to be broad enough to catch what might be disconnected elements of a common risk."*

DAVID KENT, Vice President, Global Risk and Business Resources, Genzyme



Relationships: the underpinning of good sources

Finding good sources is often predicated on building good relationships. Getting information requires having the right contacts who will share data based on trust. Relationships must be developed and maintained with colleagues throughout the organization, peers at other companies, law enforcement, government officials, and personnel from industry associations, in order to cultivate useful sources of intelligence.

The team needs to collect enough information to perform meaningful analysis but the goal is not to collect data on everything from everywhere. The team has to prioritize based on the threat model and information they are trying to protect, as well as the total costs of data collection and use. In addition, it should be recognized that often the team has to begin an analysis with incomplete information.

SOURCES OF CYBER-RISK DATA

7 GOVERNMENT SOURCES

Type of Source	Examples	Data Provided	Key Factors
Computer Emergency Response Agencies	• U.S.: U.S.- CERT • Europe: CERT-FI (Finland), DFN-CERT (Germany), GOVCERT.NL (Netherlands), GovCERT and CPNI (UK) • India: CERT-In • Global: FIRST • Australia: AusCERT	• Reports, advisories, and alerts on threats and vulnerabilities • Best practices and security tips • Attack indicators*	• Threat data is mainly non-automated via emails and web postings • Vulnerability data often in machine-readable formats • Some CERTs are membership-based
Federal Government Security Agencies	• U.S.: DHS, NSA • UK: GCHQ, Home Office • Germany: BSI • Australia: DSD	• Reports, advisories, and alerts on threats and vulnerabilities • Threat briefings • Attack indicators	• Publicly available data on the threats is mainly non-automated via web postings • Vulnerability data sometimes provided in machine-readable formats • Indicator databases starting to be available (DHS) • Classified data cannot be shared widely • Unclassified briefings provided to certain enterprises
Law Enforcement	• Local police: cyber-crime offices • National police such as: FBI/InfraGard (U.S.), SOCA (UK), BKA (Germany) • International: INTERPOL	• Cyber-crime reports • Data on attack techniques • Validation of criminal activity • Attack indicators	• For specific information (versus public reports) need to navigate through the system to find good contacts • Mostly non-automated data

**Attack indicators include: black-listed IP addresses, domain names, command and control servers, phishing sites, email addresses, file names, binaries, and malware signatures.*

8 INDUSTRY ASSOCIATIONS AND NETWORKS

Type of Source	Examples	Data Provided	Key Factors
Information-Sharing Associations	• U.S. sectorial: ISACs such as the FS-ISAC and IT-ISAC, and ES-ISAC • U.S. Energy: EnergySec • U.S. Defense Industrial Base: DCISE • U.S. public/private: ESF • Europe: ENISA • UK: WARPs, UKPA • Global IT industry: ICASI • Regional: PRISEM, ACSC • Vendor: RSA eFraudNetwork	• Reports, advisories, and alerts on threats and vulnerabilities • Best practices and security tips • Attack indicators	• Mainly non-automated data provided via emails and web postings • Some associations are moving towards providing some automated data feeds • Typically membership-based with range of fees
Informal Information-Sharing Groups	Informal networks of security professionals from a local area or a vertical industry	• Information on threats and vulnerabilities	• Mostly face-to-face meetings
Peers at Other Companies	Members of the security, incident-response, and/or intelligence teams	• Best practices and security tips • Validation of similar activity on their networks • Attack indicators	• Mainly non-automated data shared via personal contact, phone calls, and emails • Presentations at conferences
Security Researchers	Academic or industry-supported	• Vulnerability information • Potential threat scenarios • Defensive methods	• Mainly information provided through personal contact, networking events, and conferences

9 COMMERCIAL SOURCES

Threat Feeds	ZeusTracker, Bit9, SANS Internet Storm Center, Malware Domain List, Stopbadware, Team-Cymru, IPtrust.com, RSA AFCC	• Attack indicators	• Typically subscription fee-based or pay-per-view • Machine-readable data in various formats • Threat feeds are integrated with technology platforms such as threat-detection and security-intelligence systems
Threat-Intelligence Research Services	Cyveillance, iDefense, iSightPartners, RSA CyberCrime Intelligence Service, Mandiant	• Data on specific attackers and their techniques as well as investigations of compromise	• Various types of engagements • Delineate services to be provided via a statement of work

10 EXTENDED ENTERPRISE SOURCES

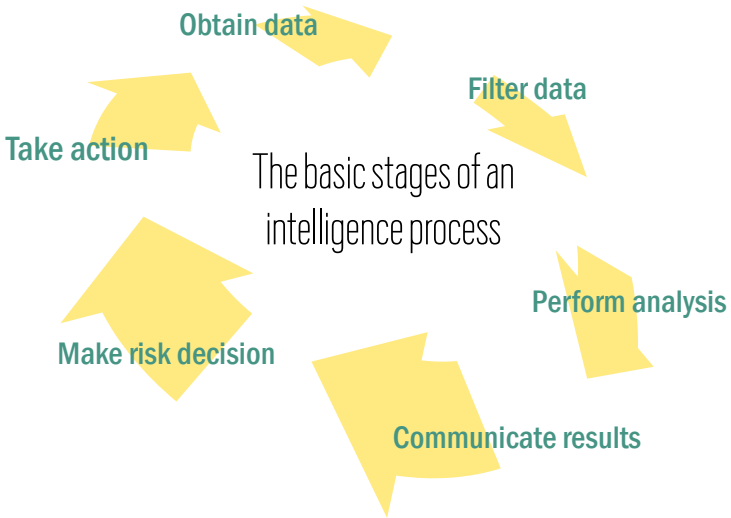
Business Partners	• Supply chain • Business-process outsourcers • Service providers	• Best practices and security tips • Validation of similar activity on their networks • Attack indicators	• Mainly non-automated data via personal contact, phone calls, and emails • Include information-sharing obligations in contract
Managed Security Service Providers	• AT&T • Verizon	• Validation of similar activity on other networks	• Include information-sharing obligations in contract

Type of Source	Examples	Data Provided	Key Factors
11 ORGANIZATION'S INTERNAL SOURCES			
Employees, Contractors	• Enterprise employees • Resident contractors	• Observations of suspicious activities and/or incidents	• Employee awareness required • Automated mechanism required for handling volumes of reporting • Hot line
Executives	Departments such as finance, corporate strategy, business lines	• Discussions regarding business strategies and associated risks	• Executive awareness required • Information-sharing working groups and/or forums
IT and Security Infrastructure	Business applications, GRC systems, SIEM systems, network-monitoring systems	• Logs, alerts, and reports	• Machine-readable data • Advanced analysis tools often used to amalgamate data from these sources, for example to baseline normal activity

Step 5: Define a Process

For designing a cyber-risk intelligence program, the goal is a standardized methodology that produces actionable intelligence and ensures an appropriate response. Given the nature of intelligence, the process will need to work on both a tactical and strategic timescale. Certain information such as precise, real-time attack indicators will call for immediate action while other information such as knowledge of protracted attack techniques will require longer-term defensive initiatives. Intelligence needs to inform not only day-to-day operations but also provide a more strategic outlook over a period of years.

The diagram below is an illustration of a basic process for collecting data, extracting meaning, making risk decisions, and taking action. It is set up as a feedback loop so as knowledge is gained, it's fed back into the system. For example, if an action is taken to modify security controls, data on the updated security posture becomes new input data.



The basic stages of a process can be described as follows:

- Obtain data
  - Input data from external and internal sources is collected and indexed.
- Filter data
  - Data that is irrelevant, not credible, or too vague is removed.
  - Irrelevant data could be exploits involving technologies not used or attacks targeting assets that are not owned by the organization.
  - Data that is judged not credible could be based on previous experience with that source providing unreliable data or on receiving conflicting data.
- Perform analysis
  - Various pieces of data are amalgamated, correlated, and studied to determine how they all relate.
  - Analysis is typically a mix of manual and automated techniques (from white-boarding to interactive analytics).
  - Analyses include an initial assessment of the risk and options for risk mitigation.
- Communicate results
  - Ideally, exigent risks are surfaced to an automated dashboard for immediate attention by the Security Operations Center (SOC). *For example, if the analysis finds evidence within the IT environment of outbound traffic to an adversary's command and control server.*

- For communicating the results of ongoing analyses, an effective method is a system of regular intelligence briefings to key stakeholders.
  For example, the results of analysis may include intelligence on the intent of adversaries, potential opportunities available to them, and/or the capabilities they may have to exploit the opportunities.
- Briefings can be provided to different audiences at various time intervals.
  For example, daily briefings to the security team, weekly briefings to IT, monthly briefings to an executive risk committee, and quarterly briefings to executive leadership.
- Besides regular briefings, out-of-band procedures for communicating high risks are also needed.
  For example, proof of an imminent attack affecting critical systems might be communicated right away versus indications of a possible future attack which would be included in a regular threat briefing.

→ Make risk decision

- Ideally, for exigent risks, a protocol has been set for the SOC to make a risk determination and take immediate action.
- For other critical risks, once they are identified and communicated by the intelligence team, depending on the risk, other stakeholders (such as IT, business/mission owners, risk officers, executives) may weigh in on the risk assessment and options for mitigation.
- A risk calculation is performed considering the potential impact to the organization versus the costs to mitigate the risk.
- A decision is made regarding actions to be taken for each specific risk.

→ Take action

- The action required will range from reconfiguring security tools to overhauling network architecture and implementing new security controls.
- A few examples of possible actions that could be taken in response to intelligence include:

  Change a firewall rule across the organization.

  Develop a new correlation rule for the SIEM.

  Rein-in access privileges for a set of critical assets.

  Segment the network to isolate certain critical assets.

  Implement encryption for certain critical business processes.

The cyber-intelligence team cannot work in isolation. The security-management process should delineate who is involved at every stage. For example, the team must have the right relationships across the organization to coordinate a response to the intelligence. It will require relationships with members of SOC, network operations, system administrators, and/or business lines, and so on. Certain situations may call for outside expertise such as malware forensics if not available in-house. Having a flexible protection platform is also essential for rapid response. For example, with a centralized management architecture, large-scale firewall changes could be made quickly across hundreds of control points.

Operational responsibility for information security is typically dispersed throughout an organization but center-led by the Chief Information Security Officer (CISO). Therefore, creating an effective cyber-risk intelligence process will require bridging between organizational and data-management silos. It may be possible to leverage existing systems for facilitating data flows. For example, some organizations have set up a common database for all information- and physical-security incidents and/or have built knowledge-management and workflow processes for an enterprise risk-management program. An intelligence program could piggy-back on these types of efforts. However new technologies may also be required.

"The process needs to be fast, fluid, and enable dynamic response – not be fixed, rigid, or stratified. If the goal is for the organization to outmaneuver cyber adversaries, the cyber-intelligence team can't get bogged down by bureaucracy."

WILLIAM BONI
Corporate Information Security Officer (CISO), VP Enterprise Information Security, T-Mobile USA

If you have intel on a threat which has not yet materialized into an attack, there may be a tendency to say, 'Well, it has not happened to us so far, why do we need to worry about it now?' Response prioritization becomes very important and at the same time very challenging when it's a prospective threat."

VISHAL SALVI
Chief Information Security Officer
and Senior Vice President,
HDFC Bank Limited

Step 6: Implement Automation

To facilitate the intelligence process, organizations should look at opportunities for automation. A cyber-risk intelligence program inherently involves "big data." For example, to keep up on current threats, an organization will probably be collecting cyber-attack indicators from as many reliable sources as possible. To gain insights into its entire IT environment, it will be amassing logs and full packet information from relevant systems and network devices across the organization.

The whole point of the intelligence effort is to correlate and analyze data from multiple sources in order to understand the threats and the organization's security posture against them. This program can easily accumulate vast amounts of data. It's simply not realistic to have humans handle all of it at every step. An effective program necessitates automation and planning the storage, analytic, and network architectures.

It is important to recognize, though, that implementing technology solutions does not equal developing an intelligence-analysis process. Automated systems make the large data sets manageable and accessible so that the analysts can more easily see relationships among disparate data types, identify connections, and notice patterns of activity forming; but they do not fulfill the requirements for the complete analysis.

Although there is no silver-bullet technology for a cyber-risk intelligence program, there are several technologies available today for automating elements of data collection, analysis, and management. There are four general areas in which leading organizations make technology investments for a cyber-risk intelligence program:

a. Automating the consumption of threat feeds

The format of cyber-attack indicators is sometimes a list of unstructured data. When it is delivered in a non-automated fashion, such as via email text or website posting, it has to be processed manually. For example, an analyst will enter it into a database to check the IT infrastructure for these signs of attack.

Fortunately, there are a growing number of government, industry-association, and commercial sources that provide automated threat feeds: machine-readable data such as comma-delimited ASCII. The technologies used to consume automated threat feeds are typically security information and event management (SIEM) systems, network-monitoring and forensics systems, and/or security-intelligence databases.

One of the challenges in working with automated threat feeds is that there is no standardization for how the content is organized. The order of data fields varies from one feed to the next. Therefore,

"You get a fire hose of information from potentially thousands of sources and need somewhere to put it – ideally a platform that enables fast searches in an un-normalised form, rapid analysis, and automated anomaly detection."

ROBERT RODGER,
Group Head of Infrastructure Security,
HSBC Holdings plc

"One of the biggest problems in the world of intelligence is that you quickly drown in data. You get masses of data, but you have to be able to derive knowledge from it, make it relevant and actionable – that takes good tools and better still excellent analysts."

PROFESSOR PAUL DOREY,
Founder and Director, CSO Confidential and
Former Chief Information Security Officer, BP

the data may need to be parsed before it is readable by a particular technology platform. However, there are aggregated threat-feed services that provide indicators from multiple sources, pre-process the data, and parse it into a consistent format.

Another way that organizations can integrate automated threat feeds into their current environment is by implementing technology platforms such as routers, anti-malware products, and adaptive-authentication solutions that automatically contain threat data.

b. Automating the collection of employee observations

Collecting information from thousands of employees across a large global enterprise is ultimately not feasible without some way to automate the process. If the intelligence team is interested in gathering data from employees on potential or actual incidents, reporting methods such as emails or phone calls to security simply do not scale. Increasingly, organizations implement knowledge-management systems for employees to report events to the intelligence team. These systems enable searching based on various parameters and can be customized to provide alerts. The main challenge will be getting employees to understand what events are to be reported and consistently use the system for reporting.

c. Automating log analysis and full packet capture

An area of focus for many cyber-risk intelligence programs is gaining visibility into the organization's own internal IT environment. Security-data analytics has emerged as an innovative approach modeled on business-intelligence systems, which process massive amounts of customer data to spot fraud or business opportunities. "Security intelligence" systems process data such as end-user behavior and system activity to spot cyber-attack indicators. The concept is to aggregate data logs and full packet data, such as application-access logs or network data that many organizations already routinely collect, then perform various functions such as baseline normal activity, discover anomalies, create alerts, develop trending, and even predict incidents.

d. Automating the fusion of data from multiple sources

Some organizations are taking an even bigger-picture view and amalgamating cyber-risk data from both internal and external sources into a "fusion center" or "security-data warehouse." The idea is to merge current data from the organization's IT and business environments with the latest information on threats into one large-scale analysis engine to achieve precise situational awareness.

The vision is a "big data" view of information security which will enable security teams to have real-time access to the entirety of information relevant to security risks. Advances in database technologies, data-storage systems, computing power, and analytics are helping organizations to realize this vision.

5 No Organization is an Island

Improving Information Sharing

"Sharing information is not the end state. The end state is to get actionable information that will help improve corporations' and governments' cyber-security posture and continually raise the bar."

WILLIAM PELGRIN, President & CEO, Center for Internet Security; Chair, Multi-State Information Sharing and Analysis Center (MS-ISAC); and Immediate Past Chair, National Council of ISACs (NCI)

Sharing cyber-risk intelligence and defensive strategies has become imperative in today's threat landscape. No organization can realistically sit in isolation and still be able to defend itself.

One of the most propitious aspects is the exchange of cyber-attack indicators. If large communities of organizations could readily and continuously exchange data on current attack methods, it would seriously impede attackers' operations. With an online early-warning system, organizations under attack could share attack profiles, so that others could prepare to defend themselves against similar (or even the very same) attacks.

Most information-security professionals have established informal networks of trusted contacts at other companies. Informal networks can be invaluable; they are often the most frequent way organizations share information. However, informal networks do not enable information sharing on a large scale.

For achieving large-scale exchange of information, there are a growing number of industry or government-led information-sharing initiatives as well as public/private partnerships. A few examples from various geographies are provided in the chart below.

12. EXAMPLES OF INFORMATION-SHARING INITIATIVES

Geography	Information sharing initiatives
International	• Forum of Incident Response and Security Teams (FIRST) • Industry Consortium for Advancement of Security on the Internet (ICASI)
National	• Computer Emergency Response Teams (CERTs) throughout Europe and Asia • Warning, Advice and Reporting Point (WARP) and CESG in the UK • Sectorial Information Sharing and Analysis Centers (ISACs), EnergySec, U.S.-CERT, Defense Industrial Base Collaborative Information Sharing Environment (DCISE), and Enduring Security Framework (ESF) in the U.S.
Regional	• Public Regional Information Security Event Management (PRISEM) in Washington • Advanced Cyber-Security Center (ACSC) in Massachusetts

"You have to invest time in being an active member of an external network. To fight threats requires data. Other companies need to be willing to share data with you."

DR. MARTIJN DEKKER
Senior Vice President, Chief Information Security Officer, ABN Amro

Models of operation and profiles of members vary, but all of these entities have similar information-sharing goals. Also, since some are relatively new – formed in the past few years – they continue to evolve. Some entities have already become effective channels for information exchange. Other entities have not yet reached a critical mass of participation by all members.

There are many challenges to creating information-sharing mechanisms. Participation is often hindered by a lack of resources. As well, the confidential nature of the information makes it tough to share. Organizations have good reasons not to want others to know how they are being targeted by cyber adversaries. Enterprises are restricted by legal issues, competitive considerations, and fears of reputation loss. Government agencies are restricted by classification requirements and national-security concerns.

Designing a way to deliver cyber-attack indicators is also enormously difficult. How does one create a system to distribute data that needs to be tightly held, yet shared with the broadest amount of people in the shortest amount of time in a form that they can immediately consume?

The good news is that, especially in the past couple of years, more organizations have started to participate and extend their contributions to information-sharing initiatives. It has often been individual companies which lead the way – deciding to make the "leap of faith" by being among the first to provide data and expecting others to follow, which spurs participation.

Groups such as the U.S. National Council of ISACs are also working to increase the number of organizations that participate, expand sector coverage, and improve cross-sector sharing. Governments in some parts of the world are actually starting to mandate participation including provisions for legal protections. For example, the government of India recently mandated participation in information exchange for the banking and critical-infrastructure sectors. There are also efforts underway to facilitate sharing mass amounts of data. Several information exchanges have pilot or production programs for providing data in machine-readable formats.

As information-sharing groups have gained experience, a set of criteria has emerged as the key ingredients for a successful exchange entity including:

- Trust among the participants
- Formalized structure (charter, board members, leadership, and professional staff)
- Adequate funding through government and/or membership fees
- Established protocol and clear rules for information sharing (what is to be shared with whom)
- Legal framework in which to share confidential information (NDA, government safe harbor)
- Standardized and reliable procedures for de-identifying confidential information to be distributed
- Streamlined mechanisms for submitting and distributing information (secure portal, encrypted email, and/or digitally signed machine-readable data)
- Genuine participation (through committed representatives and actual data contribution)

Trust and timeliness are essential components for information sharing. Within existing information-sharing groups, trust is still largely rooted in personal relationships, which does not create a sustainable system. Timeliness of information sharing continues to be a struggle as reliance is on particular individuals to post information in secure portals or securely email information. Automated data-exchange systems need to be established to remove the dependency on specific people. In addition, harmonized standards for representing attack information in machine-readable format, delivering it securely, and consuming it in real time would help to enable automation.

As cyber attacks continue to threaten enterprises and governments, more organizations will likely be motivated to invest in information sharing. An important factor paving the way is that organizations have the people, processes, and technologies in place to effectively participate in intelligence exchange.

6 Conclusion

The era of advanced threats calls for a new approach to information security. When dedicated cyber adversaries have the means and methods to elude commonly used defenses, such as signature-based detection, it is clear that conventional approaches are no longer sufficient. An intelligence-driven approach to information security can deliver comprehensive situational awareness, enabling organizations to more effectively detect and mitigate cyber attacks.

Developing a cyber-risk intelligence capability will take investments in people, process, and technology. It will challenge the information-security team to grow beyond the current skill set and to commit to a change in mind-set. And it will require not only the steadfast efforts of the security team but also broad organizational support.

The value proposition for a cyber-risk intelligence program includes improved security *and* cost-effectiveness. Defensive strategies can be precisely aimed at addressing the most significant threats and protecting the most critical assets. The security team will have the knowledge it needs to make informed risk decisions and invest in the right security controls.

Organizations must begin to recognize that having a cyber-risk intelligence capability is not just for the defense establishment and national-security agencies anymore. Government entities and corporate enterprises in many sectors must start to develop this capability in order to protect against growing threats to their operations and intellectual property.

Although many corporations have developed capabilities in competitive and market intelligence to understand their competitors and customers, most have not developed a cyber-risk intelligence program. Given that most business processes and transactions are now conducted in cyber space, activities such as fraud, espionage, and sabotage have also moved online. Cyber-risk intelligence has become a required competency to understand the online risks.

The guidance provided in this report is intended to help point the way forward. By harnessing the power of information, organizations can develop the knowledge they need to get ahead of advanced threats.

> *"If you know your attackers and what they might be capable of exploiting within your environment, you can demonstrate to your executive management that you're spending money on the right controls."*

DAVE CULLINANE,
Chief Information Security Officer and Vice President, Global Fraud, Risk & Security, eBay

7 Appendices

B *About the Security for Business Innovation Council Initiative*

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies. Yet there is still a missing link. Though business innovation is powered by information and IT systems, protecting information and IT systems is typically not considered strategic – even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or – even worse – not addressed at all. But without the right security strategy, business innovation could easily be stifled or put the organization at great risk.

AT RSA, WE BELIEVE THAT IF SECURITY TEAMS are true partners in the business-innovation process, they can help their organizations achieve unprecedented results. The time is ripe for a new approach; security must graduate from a technical specialty to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward.

RSA HAS CONVENED A GROUP OF HIGHLY successful security executives from Global 1000 enterprises in a variety of industries which we call the "Security for Business Innovation Council." We are conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports, and sponsoring independent research that explores this topic. RSA invites you to join the conversation. Go to **www.rsa.com/securityforinnovation** to view the reports or access the research. Provide comments on the reports and contribute your own ideas. Together we can accelerate this critical industry transformation.

Security for Business Innovation Report Series

THE TIME IS NOW: Making Information Security Strategic to Business Innovation

MASTERING THE RISK/REWARD EQUATION: Optimizing Information Risks to Maximize Business Innovation Rewards

DRIVING FAST AND FORWARD: Managing Information Security for Strategic Advantage in a Tough Economy

CHARTING THE PATH: Enabling the "Hyper-Extended" Enterprise in the Face of Unprecedented Risk

BRIDGING THE CISO-CEO DIVIDE

THE RISE OF USER-DRIVEN IT: Re-calibrating Information Security for Choice Computing

THE NEW ERA OF COMPLIANCE: Raising the Bar for Organizations Worldwide

WHEN ADVANCED PERSISTENT THREATS GO MAINSTREAM: Building Information-Security Strategies to Combat Escalating Threats

BUSINESS INNOVATION DEFINED

Enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or transform operations

Contributors

Top information-security leaders from Global 1000 enterprises

MARENE N. ALLISON,
Worldwide Vice President of Information Security, **JOHNSON & JOHNSON**

Prior to joining Johnson & Johnson, Marene was a senior security executive at Medco, Avaya, and the Great Atlantic and Pacific Tea Company. She served in the United States Army as a military police officer and as a special agent in the FBI. Marene is on the board of directors of the American Society of Industrial Security International (ASIS) and the Domestic Security Alliance Council (DSAC) and is President of West Point Women. She is a graduate of the U.S. Military Academy.

ANISH BHIMANI, CISSP, Chief Information Risk Officer, **JPMORGAN CHASE**

Anish has global responsibility for ensuring the security and resiliency of JPMorgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. Previously, he held senior roles at Booz Allen Hamilton, Global Integrity Corporation, and Predictive Systems. Anish was selected "Information Security Executive of the Year for 2008" by the Executive Alliance and named to Bank Technology News' "Top Innovators of 2008" list. He authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.

WILLIAM BONI, CISM, CPP, CISA, Corporate Information Security Officer (CISO), VP Enterprise Information Security, **T-MOBILE U.S.A.**

An information-protection specialist for 30 years, Bill joined T-Mobile in 2009. Previously, he was Corporate Security Officer of Motorola Asset Protection Services. Throughout his career, Bill has helped organizations design and implement cost-effective programs to protect both tangible and intangible assets. He pioneered the application of computer forensics and intrusion detection to deal with incidents directed against electronic business systems. Bill was awarded CSO Magazine's "Compass Award" and "Information Security Executive of the Year – Central" in 2007.

ROLAND CLOUTIER,
Vice President, Chief Security Officer, **AUTOMATIC DATA PROCESSING, INC.**

Roland has functional and operational responsibility for ADP's information, risk, crisis-management, and investigative-security operations worldwide. Previously, he was CSO at EMC and held executive positions with consulting and managed-services firms. He has significant experience in government and law-enforcement, having served in the U.S. Air Force during the Gulf War and later in federal law-enforcement agencies. Roland is a member of the High Tech Crime Investigations Association, the State Department Partnership for Critical Infrastructure Security, and Infragard.

DAVID KENT,
Vice President, Global Risk and Business Resources, **GENZYME**

David is responsible for the design and management of Genzyme's business-aligned global security program, which provides Physical, Information, IT, and Product Security along with Business Continuity and Crisis Management. Previously, he was with Bolt Beranek and Newman Inc. David has 25 years of experience aligning security with business goals. He received CSO Magazine's 2006 "Compass Award" for visionary leadership in the Security Field. David holds a Master's degree in Management and a Bachelor of Science in Criminal Justice.

PETRI KUIVALA,
Chief Information Security Officer, **NOKIA**

Petri has been CISO at Nokia since 2009. Previously, he led Corporate Security operations globally and prior to that in China. Since joining Nokia in 2001, he has also worked for Nokia's IT Application Development organization and on the Nokia Siemens Networks merger project. Before Nokia, Petri worked with the Helsinki Police department beginning in 1992 and was a founding member of the Helsinki Criminal Police IT- investigation department. He holds a degree in Master's of Law.

DAVE MARTIN, CISSP, Chief Security Officer, **EMC CORPORATION**

Dave is responsible for managing EMC's industry-leading Global Security Organization (GSO) focused on protecting the company's multibillion-dollar assets and revenue. Previously, he led EMC's Office of Information Security, responsible for protecting the global digital enterprise. Prior to joining EMC in 2004, Dave built and led security-consulting organizations focused on critical infrastructure, technology, banking, and healthcare verticals. He holds a B.S. in Manufacturing Systems Engineering from the University of Hertfordshire in the UK.

TIM McKNIGHT,
CISSP, Vice President and Chief Information Security Officer, **NORTHROP GRUMMAN**

Tim is responsible for Northrop Grumman's cyber-security strategy and vision, defining company-wide policies and delivering security to support the company. Tim received the Information Security Executive of the Year Mid-Atlantic Award and Information Security Magazine Security 7 Award in 2007. Tim has held management roles with BAE and Cisco Systems and served with the FBI. He has a Bachelor's degree and completed Executive Leadership training at the Wharton School. Tim also served as adjunct faculty at Georgetown University.

GUEST CONTRIBUTOR

WILLIAM PELGRIN, ESQ. President & CEO, Center for Internet Security (CIS); Chair, Multi-State Information Sharing and Analysis Center (MS-ISAC); and Immediate Past Chair, National Council of ISACs (NCI)

As President & CEO of CIS, Will provides leadership in establishing, implementing, and overseeing CIS's mission, goals, policies, and core principles. He is founder and Chair of MS-ISAC, which is the focal point for cyber-threat prevention, protection, response, and recovery for U.S. state, local, territorial, and tribal governments. He just finished serving his third term as chair of NCI, which works to advance the physical and cyber security of critical infrastructure and includes representation from major national industry sectors.

DAVE CULLINANE,
Chief Information Security Officer and Vice President, Global Fraud, Risk & Security, **eBay**

Dave has more than 30 years of security experience. Prior to joining eBay, Dave was the CISO for Washington Mutual and held leadership positions in security at nCipher, Sun Life, and Digital Equipment Corporation. Dave is involved with many industry associations including as current Past International President of ISSA. He has numerous awards including SC Magazine's Global Award as CSO of the Year for 2005 and CSO Magazine's 2006 Compass Award as a "Visionary Leader of the Security Profession."

DR. MARTIJN DEKKER,
Senior Vice President, Chief Information Security Officer, **ABN AMRO**

Martijn was appointed Chief Information Security Officer of ABN Amro in early 2010. Previously he held several positions in information security and IT including Head of Information Security and Head of Technology Risk Management in the Netherlands. Other positions included IT Architect, Program/Portfolio Manager, and IT Outsourcing/ Offshoring Specialist. Martijn joined ABN Amro in 1997 after completing his Ph.D. in Mathematics at the University of Amsterdam and a Master's of Mathematics at the University of Utrecht.

PROFESSOR PAUL DOREY,
Founder and Director, CSO Confidential and Former Chief Information Security Officer, **BP**

Paul is engaged in consultancy, training, and research to help vendors, end-user companies, and governments in developing their security strategies. Before founding CSO Confidential, Paul was responsible for IT Security and Information and Records Management at BP. Previously, he ran security and risk management at Morgan Grenfell and Barclays Bank. Paul was a founder of the Jericho Forum, is Chairman of the Institute of Information Security Professionals, and a Visiting Professor at Royal Holloway College, University of London.

RENEE GUTTMANN,
Chief Information Security Officer, **THE COCA-COLA COMPANY**

Renee is responsible for the information-risk-management program at The Coca-Cola Company. Previously, she was VP of Information Security and Privacy at Time Warner and Senior Director of Information Security at Time Inc. She has also held information-security roles at Capital One and Glaxo Wellcome and has been a security analyst at Gartner. Renee received the 2008 Compass Award from CSO Magazine and in 2007 was named a "Woman of Influence" by the Executive Women's Forum.

FELIX MOHAN,
Senior Vice President and Chief Information Security Officer, **AIRTEL**

At Airtel, Felix ensures that information security and IT align with changes to the risk environment and business needs. Previously, he was CEO at a security-consulting firm, an advisor with a Big-4 consulting firm, and head of IT and security in the Indian Navy. He was a member of India's National Task Force on Information Security, Co-chair of the Indo-U.S. Cybersecurity Forum, and awarded the Vishisht Seva Medal by the President of India for innovative work in Information Security.

ROBERT RODGER,
Group Head of Infrastructure Security, **HSBC HOLDINGS plc**

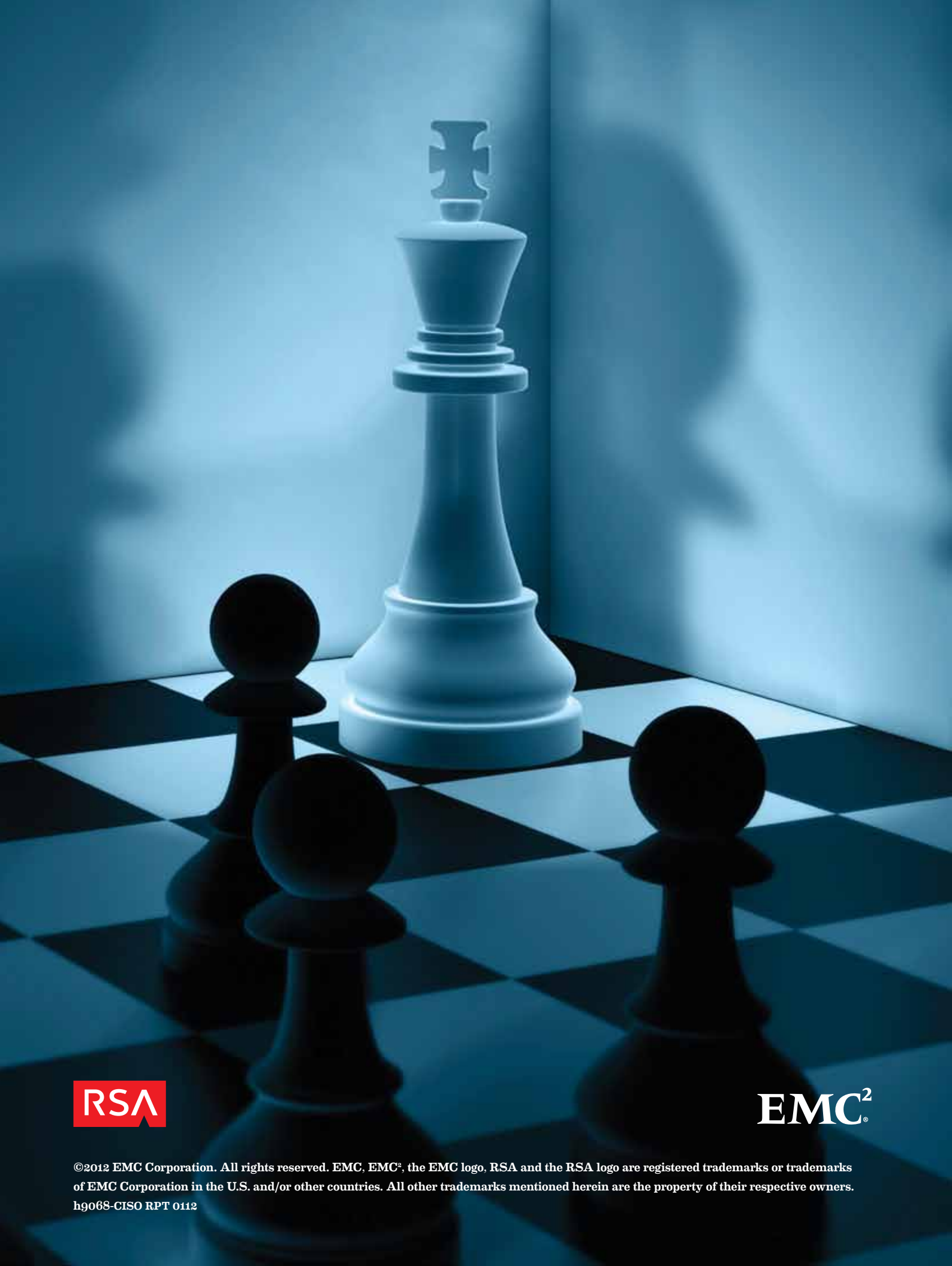
Bob has been with HSBC Bank since 2004. He is responsible for Infrastructure (IT) Security and IT Security Architecture for the Group. Previously, Bob was Head of IT Security at Bank of Bermuda and worked for the Bank of Scotland Group in IT Security consulting roles. He has over 16 years' experience in banking IT security, designing and implementing end-to-end security solutions for internal and external-facing applications. He holds a B.Sc.(Hons) in Information Technology with applied Risk Management.

RALPH SALOMON,
Vice President, IT Security & Risk Office, Global IT, **SAP AG**

Ralph is responsible for developing and maintaining the global IT security strategy and operational IT security at SAP worldwide. His many accomplishments include integration of Security, Quality, and Risk Management and improvements in IT Service and Business Continuity Management, which led SAP to achieve ISO 27001 certification and to become the first German company to be BS25999 certified. Prior to SAP, Ralph worked at KPMG as an IT Security, Quality, and Risk Management advisor and auditor.

VISHAL SALVI, CISM,
Chief Information Security Officer and Senior Vice President, **HDFC BANK LIMITED**

Vishal is responsible for driving the Information-Security strategy and its implementation across HDFC Bank and its subsidiaries. Prior to HDFC, he headed Global Operational Information Security for Standard Chartered Bank (SCB) where he also worked in IT Service Delivery, Governance, and Risk Management. Previously, Vishal worked at Crompton Greaves, Development Credit Bank, and Global Trust Bank. He holds a Bachelor's of Engineering degree in Computers and a Master's in Business Administration in Finance from NMIMS University.



h9068-CISO RPT 0112